27 April 2017

Data Security and Data Protection in the context of TCSPs

This document sets regulatory practices desirable for the protection of client data in TCSPs, in support of the Standard established by the Group of International Finance Centre Supervisors ("GIFCS").

Key Objective

The key objective of the Standard in respect of data security is to protect customers against the loss of data. This includes protection against theft, unauthorised access, and the accidental loss or destruction of data.

The Standard also refers to the more European-based concept of data protection, by citing data protection principles. This aspect of the Standard should be simpler for jurisdictions which have European-style data protection laws because data protection principles will be familiar and separately enforced across all types of business.

Principal themes of data security

The principal themes of data security can be grouped under the headings of security provisions and data protection.

- ***Security provisions:*** Regulations should secure the protection of client data. Regulations should provide that TCSPs must have suitable arrangements to protect data from:-
    - Theft or unauthorised access; and
    - Loss or destruction – including backup and disaster recovery.

Cyber-security is the principal, though not the only, threat to client data. Past incidents have shown that hacking and breaches of cyber security can lead to breaches of data security on a previously unimaginable scale.

Regulators might address cyber security as a theme within risk management and internal control.

- ***Data protection:*** Regulations should address TCSPs' standards of data protection. Data protection legislation can reinforce data security requirements directly, through its own statutory requirement to keep data secure. Where data protection legislation is not in force, the application of data protection principles can also assist through:-
    - Measures to establish that data is not excessive;
    - Measures to destroy data that is no longer required;
    - Limitations on access and use; and
    - Controls over transfer to other parties and jurisdictions.

Where a jurisdiction has data protection legislation in place that incorporates the established principles, it is for the data protection authority of that jurisdiction to enforce those principles rather than the financial services regulator. The financial services regulator would typically address data protection under the headings of corporate governance and risk management rather than duplicating the data protection regime in the regulatory framework.

Where there is no equivalent legislation it may be appropriate for a financial services regulator to supervise compliance in this area.

Many GIFCS member jurisdictions do not have data protection legislation. However, many of the data protection principles cited are relevant to data security, either directly or indirectly.

Other considerations and safeguards

In addition to the principal themes of data security and data protection, other safeguards include provisions relating to outsourcing:

- ***Outsourcing:*** Regulators should consider the Standard's provisions on outsourcing and how data security may be affected by any proposal for outsourcing which involves access to or transfer of client data.
- ***Reliance on technology:*** IT enables the copying and transfer of large volumes of data quickly and unobtrusively. IT also enables new methods of bypassing security and accessing confidential material. However, many regulators do not have the specialist knowledge of IT data security to conduct a detailed assessment of data security.
- ***Security awareness:*** Regulators should consider:-
    - Whether there are opportunities to draw attention to specific risks relating to data security arising from developments in their jurisdiction or elsewhere.